Office of Inspector General

U.S. Department of Labor
Office of Information Technology Audits

Government Information Security Reform Act Evaluation of the Bureau of Labor Statistics' International Price Program

FINAL REPORT

This review was performed by KPMG LLP under contract to the Office of Inspector General, and, by acceptance, it becomes a report of the Office of Inspector General.

/s/
Assistant Inspector General for Audit

Report Number 23-01-005-11-001
Issued: September 24, 2001

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Department of Labor (DOL), Office of Inspector General (OIG), contracted with KPMG LLP, to assist with conducting an independent evaluation of information security programs and practices within DOL's Bureau of Labor Statistics' (BLS) International Price Program.† This evaluation was conducted pursuant to guidance articulated by the Office of Management and Budget (OMB) and the National Institute for Standards and Technology (NIST), in order to satisfy OIG reporting requirements under Title X, Subtitle G of the 2001 Defense Authorization Act, the Government Information Security Reform Act (GISRA).

The purpose of this task was to assess the IPP security program and its major application, the International Price Program (IPP) Application System. The evaluation team was guided in their assessment by standards and policies set forth by NIST in support of the Security Act, as well as other key authoritative sources of guidance for accessing Federal information security programs.

Positive Security Control Observations

BLS/IPP has taken several steps to improve the overall quality of their security program. In January 2000, BLS externally contracted an independent evaluation of IPP and the generation of a Sensitive Application Security Review (SASR) Report of Findings that identified the results of the review. In conjunction with and in response to the SASR, BLS/IPP developed the IPP Major Application Security Plan (MASP) in order to document the security requirements of the BLS IPP Application System as well as the controls in place or planned for implementation to meet those requirements.

Additionally, the IPP Configuration Management (CM) Branch has recently adopted the newly issued DOL Systems Development Life Cycle Management Manual (SDLCMM) as its methodology for all Information Technology (IT) initiatives. Finally, BLS has implemented a detailed and wide-ranging set of review techniques for assessing the operational effectiveness of and compliance with controls in place in IPP. These observations are described in detail on page 8.

† The International Price Program (IPP) is distinguishable from the International Price Program Application System (IPP Application System) in that the IPP encompasses all processes and resources, automated and manual, IT-related and non-IT related, logical and physical, that contribute to the Program mission. A component of the Program is the IPP Application System. When referring to the Program, the identifier "IPP" will be used. When referencing the automated information system, the identifier "IPP Application System" will be used.

Security Control Issues

There were three moderate priority findings identified during our evaluation of the IPP system, which are as follows:

1. *There are no documented procedures for appropriate handling and secure storage of potential evidence in a security-related incident and reporting.*

   We recommend BLS Management ensure that the DNIA institute and enforce guidelines that document the procedures for the handling and storage of security incident-related evidence.

2. *The completion of security training by IPP employees is not tracked.*

   We recommend BLS Management ensure that a tracking tool (e.g., a spreadsheet log or a database) to follow the completion of security training by IPP employees be implemented. BLS/IPP personnel should be able to use this tool to identify those employees who do not meet training requirements.

3. *Although schedule envelopes, which contain confidential company data, are stored in the mailroom, card key access for the entrance is not required.*

   We recommend BLS Management improve physical access controls to the mailroom, specifically to:

   - increase management oversight to ensure existing policies and procedures related to physical and logical access controls are adhered to, and
   - assess the practicality of implementing card key access to the entrance to the mailroom.

Management Response

Overall, the BLS is in agreement with the evaluation results. With the findings provided by the review team, the BLS has made further progress in addressing the remaining open recommendations.

Conclusion

We concur with BLS Management's response to the findings and recommend that they take timely corrective action to resolve the security issues identified in this report.

Security Control Issues Resolved and Closed by BLS/IPP Management during the Reporting Period.

During the course of our evaluation, the review team identified 11 additional security control issues. BLS/IPP management had taken appropriate timely corrective action to resolve and close each of the 11 issues listed below prior to the issuance of this final report. By taking appropriate timely corrective action, BLS/IPP management demonstrated that they are being proactive in addressing security over their information system assets.

1. Auditing [in the NT environment] is not configured to collect enough data on user or system actions to recreate security-related events.

2. No activities are being performed to enforce policy in place that prohibits users from accessing the Sybase10 group account directly within UNIX.

3. BLS and IPP Continuity of Operations Plans (COOP) are marked as 'Draft' and appear to be outdated.

4. The current version of the IPP COOP does not include key information regarding IPP Application System periodicities of production; voice/data line switching components; critical personnel and duties, operations and computer resources; storage medium(s) for backup tape or COOP update frequency.

5. Server Administrators do not fill out worksheets that document the completion and sign-off of BLS Security Checklists against NT and UNIX servers.

6. Components of the Major Application Security Plan (MASP) appear to be outdated and inaccurate.

7. A logging/tracking mechanism is not used to track the progress/resolution status of security-related computer incidents.

8. There are no documented procedures for tracking and following-up of issues identified during network and server security scans.

9. BLS IPP has not formally documented the processes through which such analysis, evaluation, and subsequent modification of training curricula will be performed.

10. There is no policy or procedure outlining the requirement or responsibilities for changing alarm codes to the secure room within the Press Room.

11. The door to mail processing room does not close all the way, unless pulled shut, potentially leaving the room open to unauthorized visitors.

INTRODUCTION

Background

The Bureau of Labor Statistics

The Bureau of Labor Statistics (BLS) is the principal fact-finding agency for the Federal Government in the broad field of labor economics and statistics. BLS' vision is to "be premier among statistical agencies, producing impartial, timely, and accurate data relevant to the needs of our users and to the social and economic conditions of our Nation, its workers, its workplaces, and the workers' families."

The IPP Application System

The IPP Application System is the primary source of information on price change of commodities exported from, or imported into, the international sector of the U.S. economy and publishes monthly indices on import and export prices of U.S. merchandise and services. Users depend on timely and accurate information on internationally traded goods and services and on the U.S. trade position. This information allows users to obtain an accurate measure of the U.S. deficit and supports critical economic policy decisions related to both international trade issues and analysis of domestic inflation.

The IPP Application System is processed on the IPP sub-network LAN, a distinct and separate component from the BLS General Support System (BLS-GSS). The majority of IPP users (approximately 135) are located at the National Office in the Postal Square Building (PSB) in Washington, DC. The remaining users (approximately 15) are located in the Regional offices of BLS.

Objective

The objective of this evaluation was to perform an independent evaluation of the IPP Application System security programs, through a critical examination of the programs security and security-related documents and internal correspondence, and through interviews with knowledgeable BLS/IPP personnel.

Scope and Methodology

In accordance with the GISRA, the DOL OIG contracted KPMG to serve as the OIG's independent evaluator of BLS' IPP Application System. KPMG's evaluation assessed the management, operational and technical security controls that relate to IPP. The examination was performed in BLS' Washington, D.C., national headquarters in the PSB from June 14, 2001 through August 10, 2001.

The evaluation was performed in accordance with guidance provided by OMB Memoranda 01-08, "Guidance on Implementing the Government Information Security Reform Act," dated January 16, 2001, and 01-24, "Reporting Instructions for the Government Information Security Reform Act," dated June 22, 2001.

Additionally, we used, as the framework for this evaluation, the standards and guidance contained in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-XX Draft "Self -Assessment Guide for Information Technology System," issued by NIST in March 2001. Detailed test procedures were planned and performed using this self-assessment guide, as well as the General Accounting Office's Federal Information System Controls Audit Manual (FISCAM).

The NIST Self-Assessment Guide provides a methodology for evaluating an agency information technology security program and is intended to facilitate improvement. The Guide consists of an extensive questionnaire containing specific control objectives that collectively constitute the minimum components of an effective information security program. The Guide does not establish new security standards or requirements. The control objectives in the questionnaire are drawn directly from long-standing requirements found in Federal law, regulatory and technical criteria, and guidance on security and privacy.

In addition, KPMG, LLP reviewed a Sensitive Application System Review (SASR) Report of the IPP. The SASR review was conducted by TWM, Inc., and was issued in July 2000. The review used OMB A-130 as its primary criteria. KPMG's effort was limited to reviewing and reporting on the current status of the identified findings in the SASR report.

Findings Classifications

Findings have been classified according to the control areas to which the deficient or non-existent control(s) relates. Those classifications are as follows:

- AT - Audit Trails
- LA – Logical Access
- RSC - Review of Security Controls
- SSP - System Security Plan
- SI – Security Incidents
- SATE – Security Awareness, Training, and Education
- P&ES – Physical and Environmental Security
- CP – Contingency Planning

Each finding is also referenced by the OMB Reporting Instruction to which it maps to or supports (identified in the far left Reference column).

Guide to Categorization of Findings

Findings are categorized according to the priority with which they should be addressed:

High Priority Control Findings – The identified finding presents a level of risk that requires immediate address by BLS Management. There were **no** High Priority Control Findings identified during this review.

Moderate Priority Control Findings – The identified findings present a level of risk that should be addressed by BLS Management in a timely fashion. There were **three** moderate priority control findings identified during the review.

Low Priority Control Findings – A level of risk exists within the process that is either inherent to the process or in excess of the inherent risk level by such a small margin that the address of the condition would be neither practical nor cost effective. **No** findings identified in this Report have been assigned a Low Priority.

POSITIVE SECURITY CONTROL OBSERVATIONS

BLS/IPP has taken the following steps to improve the overall quality of their security program:

- In January 2000, BLS externally contracted an independent evaluation of IPP and the generation of a Sensitive Application Security Review (SASR) Report of Findings that identified the results of the review. The scope of the SASR included the analysis and evaluation of general management and automated information system (AIS) security environment controls for the Import and Export Price Index, with an emphasis on technical, functional and operational security. OMB Circulars A-130, Appendix III and A-123 were used to perform the SASR.

- In conjunction with and in response to the SASR, BLS/IPP developed the IPP Major Application Security Plan (MASP) in order to document the security requirements of the BLS IPP Application System, as well as the controls in place or planned for implementation to meet those requirements. The MASP also identifies responsibilities and expected behaviors of all system users, as well as the structured process for implementing adequate, cost-effective security protection for the IPP Application System and its supporting infrastructure.

- The IPP Configuration Management (CM) Branch has recently adopted the newly issued DOL Systems Development Life Cycle Management Manual (SDLCMM) as its methodology for all Information Technology (IT) initiatives. The SDLCMM provides detailed guidelines for integrating security considerations into each phase of the application life cycle. Additionally, the CM Branch maintains the CM Plan, which outlines the required approvals and after-the-fact compliance activities for development efforts of any size.

- BLS has implemented a detailed set of techniques for assessing the operational effectiveness, continuity, and compliance with controls in place including:

    - biannual reviews of physical access to determine if it is commensurate with employee job status and responsibilities;
    - annual review of logical access control;
    - annual review of the MASP;
    - testing of the IPP Disaster Recovery Plan;
    - completion of BLS Security Checklist on a monthly basis by Server Administrators;

- monthly server scans performed by the Division of Network and Information Assurance (DNIA) for compliance with BLS IT Security Policy;
- annual network scans performed by the DNIA for compliance with BLS IT Security Policy;
- identification and review of user IDs inactive 60 days or greater, every 30 days; and
- weekly review of audit logs.

FINDINGS AND RECOMMENDATIONS

The following section describes the report findings and recommendations that have been identified during the fieldwork of the BLS IPP GISRA Evaluation and Review. Each finding includes a description of the condition, the cause of the condition, the criteria against which the condition was identified (e.g., NIST, GAO, OMB, etc.), the potential effects, and a recommendation to address the condition. Additionally, the related OMB requirement is referenced in order to facilitate the OIG reporting requirement process.

The tables in the subsequent section provide the conditions in detail.

Moderate Priority Findings and Recommendations

Number of Findings: 3

References	Finding and Recommendation
SI-3 **OMB Reporting Requirement II.B.5 and II.B.8**	**Condition:** The Division of Network and Information Assurance (DNIA) has not documented procedures for the appropriate handling and securing storage of potential evidence in a security-related incident. **Cause:** DNIA Management has not completed the documentation of guidelines that detail the procedures for the handling and storage of security incident-related evidence. **Criteria:** OMB Circular A-123, "Management Accountability and Control," Attachment II – Establishing Management Controls requires the institution of management controls, including the "the plan of the organization, methods and procedures . . . ensure that . . . goals are met. Management controls include processes for planning, organizing, directing, and controlling program operations." **Effect:** Procedural knowledge lies in the heads of DNIA Management. However, without documented procedures and guidance of DNIA Management, the risk exists that secondary (backup) personnel might not be able to perform the procedures properly. **Recommended Corrective Action:** We recommend BLS Management ensure that the DNIA institute and enforce guidelines that document the procedures for the handling and storage of security incident-related evidence. **Management's Comments:** The BLS concurs with the finding and recommendation and has already been at work on this issue prior to the commencement of the GISRA evaluation. **Conclusion:** We concur with Management's comment on this finding, and we recommend BLS management take timely corrective action to resolve this issue.

References	Finding and Recommendation
SATE-2 **OMB Reporting Requirement II.B.6 and II.B.7**	**Condition:** The completion of security awareness training by IPP employees is not tracked. For the following types of security training, no evidence of tracking (e.g., attendance logs, sign-in sheets, etc.) was identified: • Publication and Security Module (PSM) Training • Annual IPP Refresher Training **Cause:** Historically, IPP Training Personnel have not tracked the completion of training. **Criteria:** OMB Circular A-130, Appendix III "Security of Federal Automated Information Resources" (3) (A) (1) (b) states that "all individuals are [to be] appropriately trained in how to fulfill their security responsibilities before allowing them access to the system. Such training shall assure that employees are versed in the rules of the system, be consistent with guidance issued by NIST and OPM, and apprise them about available assistance and technical security products and techniques. Behavior consistent with the rules of the system and periodic refresher training shall be required for continued access to the system." **Effect:** Failure to track the completion of security training by IPP employees, deprives BLS of an accurate view of the workforce's security knowledge position. **Recommended Corrective Action:** We recommend BLS Management ensure that a tracking tool (e.g., a spreadsheet log or a database) to follow the completion of security training by IPP employees be implemented. BLS/IPP personnel should be able to use this tool to identify those employees who do not meet training requirements. **Management's Comments:** BLS management agrees with the finding. The issue of tracking internal security training by office, including the IPP office, is being evaluated on a Bureau-wide basis. BLS will implement a system to track security training across offices in a consistent manner.

References	Finding and Recommendation
	Conclusion: We concur with Management's comment on this finding, and we recommend BLS management take timely corrective action to resolve this issue.

References	Finding and Recommendation
P&ES-2 **OMB Reporting Requirement II.B.12**	**Condition:** Although schedule envelopes, which contain confidential company data, are stored in the mailroom, card key access for the entrance is not required. **Cause:** The entrance to the mailroom contains dual-direction swinging double doors that facilitate the transport of mail carts into the mailroom area. The current set of doors do not support the locking mechanism utilized by card key access restriction devices. **Criteria:** OMB Circular No. A-123, Management Accountability and Control, states that "access to resources and records should be limited to authorized individuals, and accountability for the custody and use of resources should be assigned and maintained." The circular further requires agencies to establish and maintain a cost effective system of internal controls to provide reasonable assurance that Government resources are protected against fraud, waste, mismanagement or misappropriation. OMB A-130, "Management of Federal Automated Information Resources" requires agencies to establish a level of security for all information systems that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in these information systems. Federal Information Processing Standards Publication 31 [FIPS PUB 31] – Guidelines for Automatic Data Processing security and risk management (pg. 6, Para. VII) states that the entity should provide physical protection. Specifically, the entity should identify critical ADP areas including the computer room, data control and conversion area, data file storage area, programmer's area, forms storage area, maintenance area, and mechanical equipment room, and then provide adequate physical protection and access control.

References	Finding and Recommendation
	Effect: Failure to control physical access to sensitive information may result in the theft, alteration or destruction of that information and resultant damage to the trust relationship with the general public and reputation with respondent organizations. **Recommended Corrective Action:** We recommend BLS Management improve physical access controls to the mailroom, specifically to: • increase management oversight to ensure existing policies and procedures related to physical and logical access controls are adhered to, and • assess the practicality of implementing card key access to the entrance to the mailroom. **Management's Comments:** The Division of Administrative Services and the Deputy Associate Commissioner for Administration will discuss the issue and notify the review team when a decision has been reached. **Conclusion:** We continue to recommend that BLS Management take timely corrective action to resolve this issue, as stated in our recommendation.

SECURITY CONTROL ISSUES RESOLVED AND CLOSED BY BLS/IPP MANAGEMENT DURING THE REPORTING PERIOD

During the course of our evaluation, the review team identified eleven additional security control issues. BLS/IPP management took appropriate timely corrective action to resolve and close each of the ten issues listed below prior to the issuance of this final report . By taking appropriate timely corrective action BLS and IPP management demonstrated that they are being proactive in addressing security over their information system assets.

References	Findings that were resolved and closed during the Reporting Period
AT-1	Auditing [in the NT environment] is not configured to collect enough data on user or system actions to recreate security-related events.
LA-1	No activities are being performed to enforce policy in place that prohibits users from accessing the Sybase10 group account directly within UNIX.
CP-1	BLS and IPP Continuity of Operations Plans (COOP) is marked as 'Draft' and appears to be outdated.
CP-2	The current version of the IPP COOP does not include key information regarding COOP storage, IPP Application System periodicities of production; voice/data line switching components; critical personnel and duties, operations and computer resources; storage medium(s) for backup tape or COOP update frequency.
RSC-1	Server Administrators do not fill out worksheets that document the completion and sign-off of BLS Security Checklists against NT and UNIX servers.
SSP-1	Components of the Major Application Security Plan (MASP) appear to be outdated and inaccurate.
SI-1	A logging/tracking mechanism is not used to track the progress/resolution status of security-related computer incidents.
SI-3	There are no documented procedures for tracking and following-up of issues identified during network and server security scans.

References	Findings that were resolved and closed during the Reporting Period
SATE-1 (Partial)	BLS IPP has not formally documented the processes through which such analysis, evaluation, and subsequent modification of training curricula will be performed.
P&ES-1	The door to mail processing room does not close all the way, unless pulled shut, potentially leaving the room open to unauthorized visitors.
P&ES-3	There is no policy or procedure outlining the requirement or responsibilities for changing alarm codes to the secure room within the Press Room.

OPEN RECOMMENDATIONS FROM THE JULY 20, 2000, TWM ASSOCIATES, INC., SENSITIVE APPLICATION SECURITY REVIEW (SASR)

The IPP Sensitive Application Security Review (SASR) performed between February-April 2000 by TWM Associates Inc. (TWM) produced 55 findings pertaining to General Controls, Application Controls, and Management Controls. The following table includes the findings number, description and status for which BLS Management has confirmed recommendations as "open." Priority ratings indicated in this table were assigned by TWM and not KPMG. KPMG's effort was limited to reviewing the current status of the identified findings in the TWM report.

SASR Finding # and Priority	Description of Finding	Status
NT-2b **(Moderate Priority)**	Authenticated users have access to files and data that they do not require to perform their duties	Open – The Foxpro-based IPP Initiation System requires the group account "TA" and resources are not currently available to replace this subsystem. The BLS is willing to accept the risk associated with this finding.
NT-6 **(Moderate Priority)**	Unnecessary communication protocols are available to network users.	Open – The DOS-based workstation that is currently used to scan monthly repricing forms requires the NetBEUI protocol. The current target for replacing this scanner is November 20, 2001.
PHYS 1-4 **(Moderate Priority)**	1. Department of Labor entry procedures through the back entrance can be improved. 2. The sign-in sheet to the Press Room during the Lockup procedure was not being used. 3. The Press Release Room is not sufficiently protected from unauthorized transmissions during the Lockup procedure. 4. A Press Room badge was hanging on the wall in the Press Room.	Open – BLS Management has identified these findings to the DOL; however, no status has been obtained. The resolution of these findings are out of BLS / IPP control.
APP-3 **(Moderate Priority)**	Laptops in the field running the PRIMO application contain IPP User	Open - BLS Management has stated that they are

SASR Finding # and Priority	Description of Finding	Status
	IDs and Passwords.	testing Smart Card and Public Key Infrastructure (PKI) solutions and are working to complete by Spring 2002.

OPEN RECOMMENDATIONS THAT WERE RESOLVED AND CLOSED FROM THE JULY 20, 2000, TWM ASSOCIATES, INC., SENSITIVE APPLICATION SECURITY REVIEW (SASR)

During the course of our evaluation, the review team confirmed that two additional security control issues which were provided in The IPP Sensitive Application Security Review (SASR) performed by TWM were resolved and closed. BLS/IPP management took appropriate timely corrective action to resolve and close these two issues listed below prior to the issuance of this final report. By taking appropriate timely corrective action BLS and IPP management demonstrated that they are being proactive in addressing security over their information system assets.

SASR Finding # and Priority	Description of Finding
NT-1 f and g **(High Priority)**	Auditing is not configured to collect enough data on user or system actions to recreate security-related events.
UNIX-3 **(High Priority)**	Auditing is not configured to collect enough user or system actions to recreate security-related events.

ACRONYMS

ADP	Automated Data Processing
AT	Audit Trails
BLS	Bureau of Labor Statistics
CAPJ	DOL Security and Privacy Capital Asset Plan and Justification
CIAO	Critical Infrastructure Assurance Officer
CIO	Chief Information Officer
CCNA	Cisco Certified Network Administrator
CM	Configuration Management
COOP	Continuity of Operations Plan
CP	Contingency Planning
CSC	Computer Security Certification
CSIRT	Computer Security Incident Response Teams
DNIA	Division of Network and Information Assurance
DOL	Department of Labor
FBI	Federal Bureau of Investigation
FIPS PUB	Federal Information Processing Standards Publication
FISCAM	Federal Information System Controls Audit Manual
FPS	Federal Protective Services
GAO	General Accounting Office
GISRA	Government Information Security Reform Act
GSA	General Services Administration
IPP	International Price Program
IS	Information System
IT	Information Technology
LA	Logical Access
LABSTAT	Labor Statistics
LAN	Local Area Network
MASP	Major Application Security Plan
MCSE	Microsoft Certified Systems Engineer
MOA	Memorandum of Agreement
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSC	National Security Council
OIG	Office of Inspector General
OMB	Office of Management Budget
OPM	Office of Personnel Management
PDD	Presidential Decision Directive
P&ES	Physical and Environmental Security
POC	Point of Contact

ACRONYMS CONTINUED

PSB	Postal Square Building
PSM	Publication and Security Module
RSC	Review of Security Controls
SASR	Sensitive Application Security Review
SATE	Security Awareness, Training, and Education
SDLCMM	Systems Development and Life Cycle Management Manual
SI	Security Incidents
SP	Special Publication
SPS-MF	Mainframe Sample Production System
SSP	System Security Plan
UDB	IPP Unified Database
WAN	Wide Area Network

U. S. Department of Labor

Commissioner for
Bureau of Labor Statistics
Washington, D.C. 20212

SEP 7 2001

MEMORANDUM FOR: JOHN J. GETEK
Assistant Inspector General for Audit

FROM: KATHARINE G. ABRAHAM
Commissioner

SUBJECT: Government Information Security Reform Act (GISRA) Evaluation of BLS' International Price Program System Draft Audit Report No. 23-01-005-11-001

Thank you for the opportunity to respond to the Office of Inspector General (OIG) draft audit report regarding the Government Information Security Reform Act (GISRA) Evaluation of Bureau of Labor Statistics (BLS) International Price Program System.

Overall, the BLS is in agreement with the audit results With the findings provided by your staff, we have made further progress in addressing the remaining open recommendations.

Recommendation No. CP-2

The BLS, through discussions with the OIG contract staff, understands that this finding is now closed. The IPP COOP has been updated to reflect where the COOP is stored off-site. Information on COOP storage is in Appendix 1, labeled Information Concerning Off-site Backups. This information was provided to the OIG on August 28, 2001.

Recommendation No. SI-3

BLS has no additional comments at this time.

Recommendation No. SATE-2

The issue of tracking internal security training by office, including the IPP office, is being evaluated on a Bureau-wide basis. The BLS will implement a system to track security training across offices in a consistent manner. The OIG will be notified when a plan of action has been developed.

Recommendation No. P&ES-1

The BLS, through discussions with the OIG contract staff, understands that this finding is now closed. The doors to the mail processing room in the Postal Square Building have been repaired.

Recommendation No. P&ES-2

BLS has no additional comments at this time

Recommendation No. P&ES-3

The BLS, through discussions with the OIG contract staff, understands that this finding is now closed. Language was added to the DAS Embargoed Data Procedures document to address the requirements and responsibilities for changing alarm codes to the secure room within the Press Room (PSB 1820).

Open Recommendations from the July 20, 2000 Sensitive Application Security Review

SASR Finding (NT-2b)

BLS has no additional comments at this time.

SASR Finding (NT-6)

BLS has no additional comments at this time.

SASR Finding (PHYS 1-4)

BLS has no additional comments at this time.

SASR Finding (APP-3)

BLS has no additional comments at this time.

I appreciate your continued assistance and that of your staff in helping improve the security of BLS data. The work conducted by your audit team was quite helpful to us in identifying areas where additional security controls were needed.

If you have any questions, please contact Jesús Salinas in the Division of Management Systems on Area Code 202-691-7628.